EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

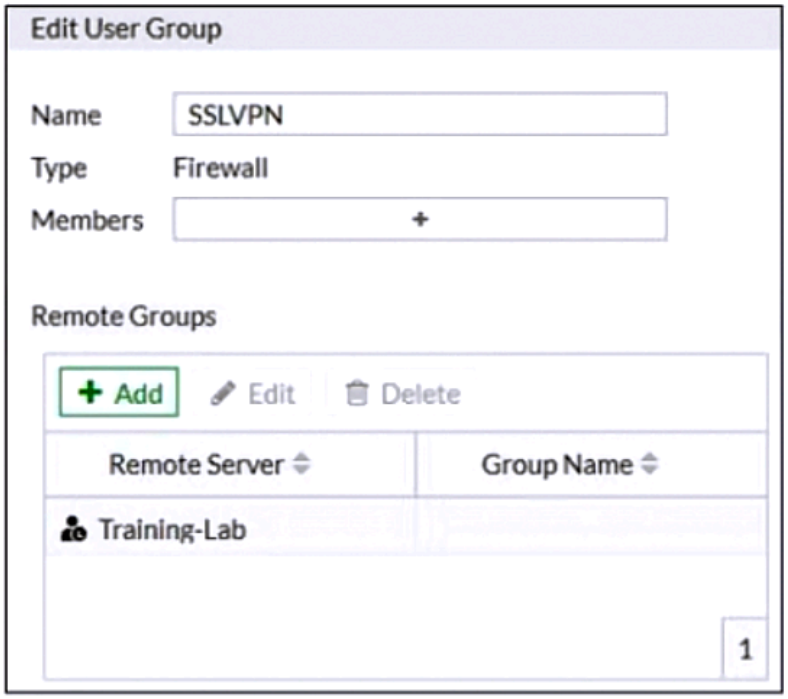
Question #1 *Topic 1*

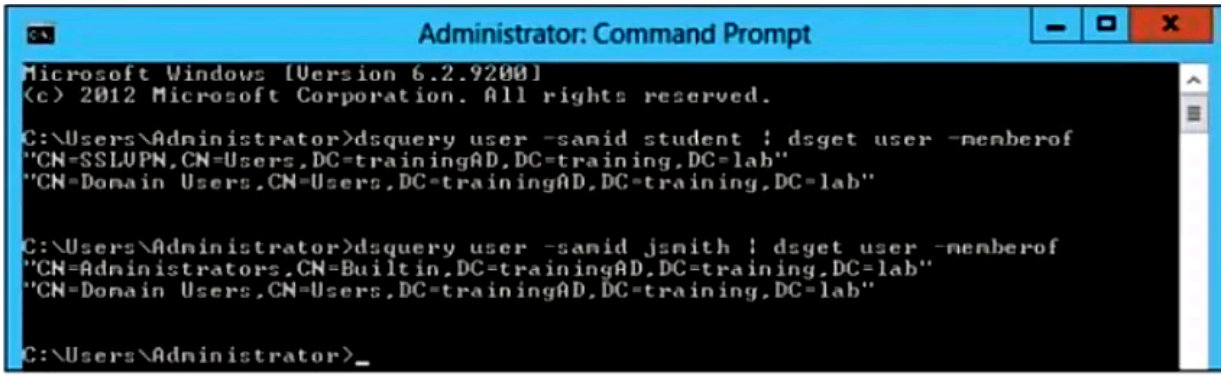
Refer to the exhibit.

Examine the FortiGate user group configuration and the Windows AD LDAP group membership information shown in the exhibit.

FortiGate is configured to authenticate SSL VPN users against Windows AD using LDAP. The administrator configured the SSL VPN user group for SSL VPN users. However, the administrator noticed that both the t and student and jsmith users can connect to SSL VPN.

Which change can the administrator make on FortiGate to restrict the SSL VPN service to the student user only?





A. In the SSL VPN user group configuration, set Group Name to CN=SSLVPN,CN=Users,DC=trainingAD,DC=training,DC=lab.

B. In the SSL VPN user group configuration, change Name to CN=SSLVPN,CN=Users,DC=trainingAD,DC=training,DC=lab.

C. In the SSL VPN user group configuration, set Group Name to CN=Domain Users,CN=Users,DC=trainingAD,DC=training,DC=lab.

D. In the SSL VPN user group configuration, change Type to Fortinet Single Sign-On (FSSO).

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

Artbrut Most Recent 2 years, 4 months ago

study guide p. 466

upvoted 1 times

Artbrut 2 years, 4 months ago

Assume A

upvoted 1 times

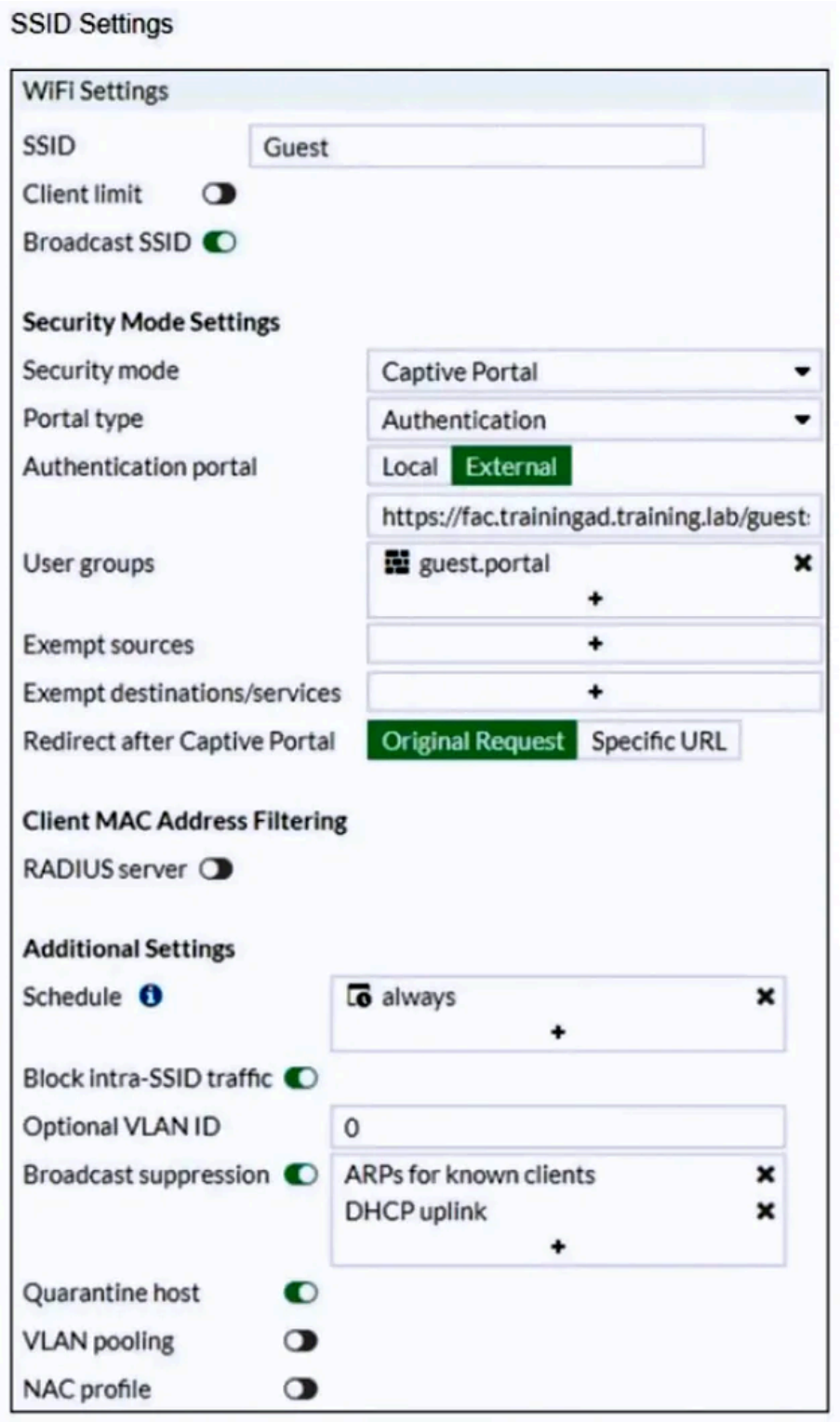
Question #2 *Topic 1*

Refer to the exhibits.

Examine the firewall policy configuration and SSID settings.

An administrator has configured a guest wireless network on FortiGate using the external captive portal. The administrator has verified that the external captive portal URL is correct. However, wireless users are not able to see the captive portal login page.

Given the configuration shown in the exhibit and the SSID settings, which configuration change should the administrator make to fix the problem?



Firewall Policy

```
config firewall policy
    edit 11
        set name "Guest to Internal"
        set uuid c5e45130-aada-51e8-ee0c-bc1204f9f163
        set srcintf "guest"
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "FortiAuthenticator" "WindowsAD"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

A. Disable the user group from the SSID configuration.

B. Enable the captive-portal-exempt option in the firewall policy with the ID 11.

C. Apply a guest.portal user group in the firewall policy with the ID 11.

D. Include the wireless client subnet range in the Exempt Source section.

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (50%) C (38%) D (12%)

jz16 Most Recent 1 year, 2 months ago

I would say D

upvoted 1 times

tonifan 1 year, 4 months ago

I choose B because guest.portal user group may be defined after CP authentication

upvoted 1 times

e8a82ad 1 year, 10 months ago

it was difficult to analize this part, but my logic says is C.

upvoted 1 times

e8a82ad 1 year, 10 months ago

it was difficult to analize this part, but my logic says is C.Scenario 1: Because on the SSID there is a field called Exempt destinations on Guide page 363 that must have a corresponding firewall policy in place, that firewall policy has ipv4 DST Addr pointing to the FortiAuthenticator (or any External server), It means if the SSID has the Excempt destination with one entry then the answer is B and you MUST enable the exempt from captive portal on the firewall policy in order to allow the traffic to the Destination server and Services like DNS, HTTP, HTTPS, ping.Scenario2: When the SSID is not including any Exempt destinations (is empty), then the Answer is C, and on this case the image shows the SSID with this field empty, as a consequence all taks are done from the Firewall policy on guide page365 using the Source user group along with its services HTTP, HTTPS, at this point you DO NOT NEED to enable the Exempt from captive portal option inside the firewall policy, otherwise all traffic will be allowed and no captive portal will be presented. As a summary on this scenario C is the correct one.

upvoted 1 times

e8a82ad 1 year, 10 months ago

Scenario 1: Because on the SSID there is a field called Exempt destinations on Guide page 363 that must have a corresponding firewall policy in place, that firewall policy has ipv4 DST Addr pointing to the FortiAuthenticator (or any External server), It means if the SSID has the Excempt destination with one entry then the answer is B and you MUST enable the exempt from captive portal on the firewall policy in order to allow the traffic to the Destination server and Services like DNS, HTTP, HTTPS, ping.

upvoted 1 times

e8a82ad 1 year, 10 months ago

Scenario 1: Because on the SSID there is a field called Exempt destinations on Guide page 363 that must have a corresponding firewall policy in place, that firewall policy has ipv4 DST Addr pointing to the FortiAuthenticator (or any External server), It means if the SSID has the Excempt destination with one entry then the answer is B and you MUST enable the exempt from captive portal on the firewall policy in order to allow the traffic to the Destination server and Services like DNS, HTTP, HTTPS, ping.Scenario2: When the SSID is not including any Exempt destinations (is empty), then the Answer is C, and on this case the image shows the SSID with this field empty, as a consequence all taks are done from the Firewall policy on guide page365 using the Source user group along with its services HTTP, HTTPS, at this point you DO NOT NEED to enable the Exempt from captive portal option inside the firewall policy, otherwise all traffic will be allowed and no captive portal will be presented. As a summary on this scenario C is the correct one.

upvoted 1 times

e8a82ad 1 year, 10 months ago

Scenario2: When the SSID is not including any Exempt destinations (is empty), then the Answer is C, and on this case the image shows the SSID with this field empty, as a consequence all taks are done from the Firewall policy on guide page365 using the Source user group along with its services HTTP, HTTPS, at this point you DO NOT NEED to enable the Exempt from captive portal option inside the firewall policy, otherwise all traffic will be allowed and no captive portal will be presented. As a summary on this scenario C is the correct one.

upvoted 1 times

cestraining 2 years, 1 month ago

just a note guys - I wrote today and got only about 15 questions from this guide. had to figure all the other questions out - a lot of FortiAuthenticator and wireless questions were new.

upvoted 2 times

BBell29128 2 years, 2 months ago

Which study guide are you guys referring to in the discussion? I've reviewed the guide available on the Fortinet Training page for the online LAN Edge course and the page numbers don't line up.

upvoted 1 times

Artbrut 2 years, 4 months ago

Revert! C is right as per page 365 study guide! Read pages 363-365!

upvoted 1 times

Artbrut 2 years, 4 months ago

study guide p. 363plus page 364!

upvoted 1 times

Artbrut 2 years, 4 months ago

Selected Answer: B

study guide p. 363

upvoted 1 times

Artbrut 2 years, 4 months ago

plus page 364!

upvoted 1 times

aandreou020 2 years, 6 months ago

Answer B Study Guide P363

upvoted 1 times

kinge2 2 years, 6 months ago

study guide page 363 - if using external captive portal configure policy and exempt web traffic to external captive portal

upvoted 2 times

ZengIT 2 years, 6 months ago

Using B will ignore the portal entrance,The correct setting should be to set the source of ID11 policy to the Guest.portal GroupIncorrect, The portal cannot be seen, we havent reached authentication yet, the portal address needs to be exempt, so it can be seen first. B is the Answer

upvoted 2 times

ZengIT 2 years, 6 months ago

Selected Answer: C

Using B will ignore the portal entrance,The correct setting should be to set the source of ID11 policy to the Guest.portal Group

upvoted 2 times

jimmyjampot 2 years, 1 month ago

Incorrect, The portal cannot be seen, we havent reached authentication yet, the portal address needs to be exempt, so it can be seen first. B is the Answer

upvoted 1 times

Question #3 *Topic 1*

Which two statements about the MAC-based 802.1X security mode available on FortiSwitch are true? (Choose two.)

A. FortiSwitch authenticates a single device, and opens the port to other devices connected to the port.

B. FortiSwitch authenticates each device connected to the port.

C. It cannot be used in conjunction with MAC authentication bypass.

D. FortiSwitch can grant different access levels to each device connected to the port.

Suggested Answer: *B, D*

Official Answer: BD

Community vote distribution



Artbrut Most Recent 1 year, 11 months ago

B and D, study guide p. 267

upvoted 1 times

mollyk70 1 year, 11 months ago

apologies, BD correct as its asks about MAC based A incorrect as this is port based B correct D correct Study guide 267

upvoted 1 times

mollyk70 1 year, 11 months ago

A is correct - P267 specifically states FS authenticates a single host and opens the port to other devices behind that port. D is correct, P267 Study guide, specifically states if you want to auth each device behind a port and optionally grant each device with a different access level based on credentials provided, then MAC based is requiredA is only correct with Port-based security mode. The question states MAC-based security mode.

upvoted 1 times

mollyk70 1 year, 11 months ago

A is correct - P267 specifically states FS authenticates a single host and opens the port to other devices behind that port. D is correct, P267 Study guide, specifically states if you want to auth each device behind a port and optionally grant each device with a different access level based on credentials provided, then MAC based is required

upvoted 1 times

Artbrut 1 year, 11 months ago

A is only correct with Port-based security mode. The question states MAC-based security mode.

upvoted 1 times

kinge2 2 years ago

page 267 of study guide

upvoted 1 times

Question #4 *Topic 1*

A wireless network in a school provides guest access using a captive portal to allow unregistered users to self-register and access the network. The administrator is requested to update the existing configuration to provide captive portal authentication through a secure connection (HTTPS). Which two changes must the administrator make to enforce HTTPS authentication? (Choose two.)

A. Create a new SSID with the HTTPS captive portal URL.

B. Enable HTTP redirect in the user authentication settings.

C. Disable HTTP administrative access on the guest SSID to enforce HTTPS connection.

D. Update the captive portal URL to use HTTPS on FortiGate and FortiAuthenticator.

Suggested Answer: *B, D*

Official Answer: BD

Community vote distribution



tonifan Most Recent 1 year, 4 months ago

I agree B and D. https://community.fortinet.com/t5/FortiGate/Technical-Tip-Using-secure-authentication-HTTPS-on-a-FortiGate/ta-p/192486

upvoted 1 times

Artbrut 1 year, 10 months ago

As A and C are far-fetched and per study guide p. 367 and following pages

upvoted 1 times

kinge2 1 year, 11 months ago

BD correct as per https://community.fortinet.com/t5/FortiGate/Technical-Tip-Using-secure-authentication-HTTPS-on-a-FortiGate/ta-p/192486

upvoted 1 times

Question #5 *Topic 1*

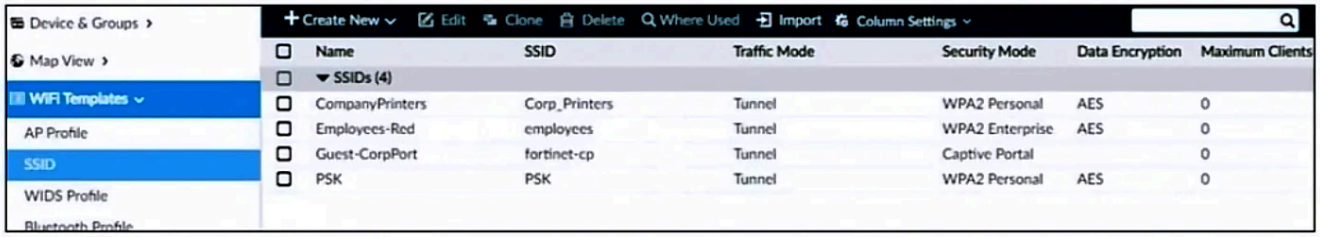
Refer to the exhibit.

The exhibits show the wireless network (VAP) SSID profiles defined on FortiManager and an AP profile assigned to a group of APs that are supported by FortiGate.

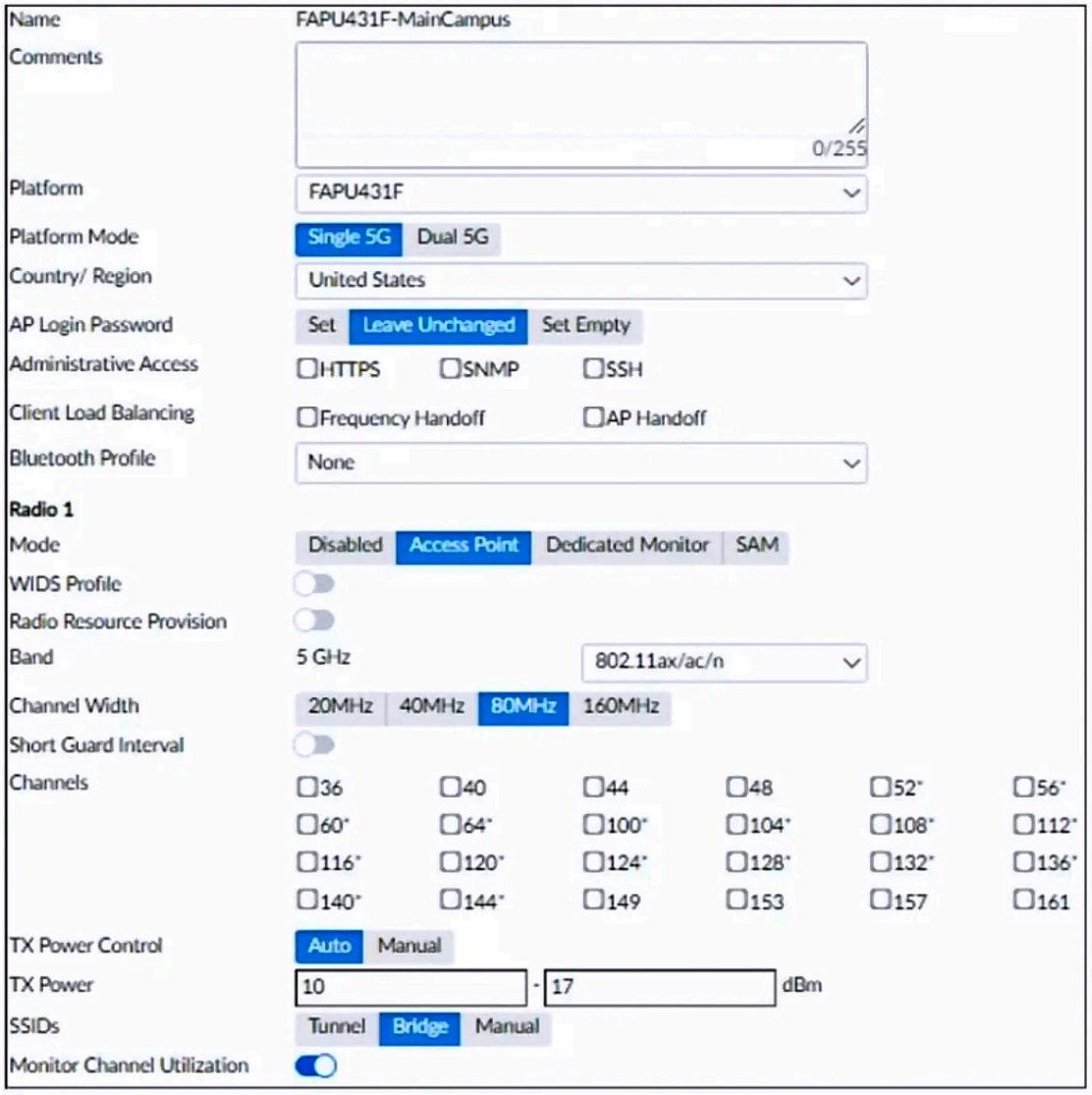
None of the APs are broadcasting the SSIDs defined by the AP profile.

Which changes do you need to make to enable the SSIDs to broadcast?

SSID Profiles



AP Profile



A. In the SSIDs section, enable Tunnel.

B. Enable one channel in the Channels section.

C. Enable multiple channels in the Channels section and enable Radio Resource Provision.

D. In the SSIDs section, enable Manual and assign the networks manually.

Suggested Answer: *D*

Official Answer: D

Community vote distribution



_zero Most Recent 1 year, 7 months ago

D is correct. B is not correct because, if any channel it was not selected the AP will use all available channels.

upvoted 2 times

Artbrut 1 year, 10 months ago

would claim "D" as per study guide p. 329

upvoted 3 times

aandreou020 2 years ago

A should be the correct answer

upvoted 4 times

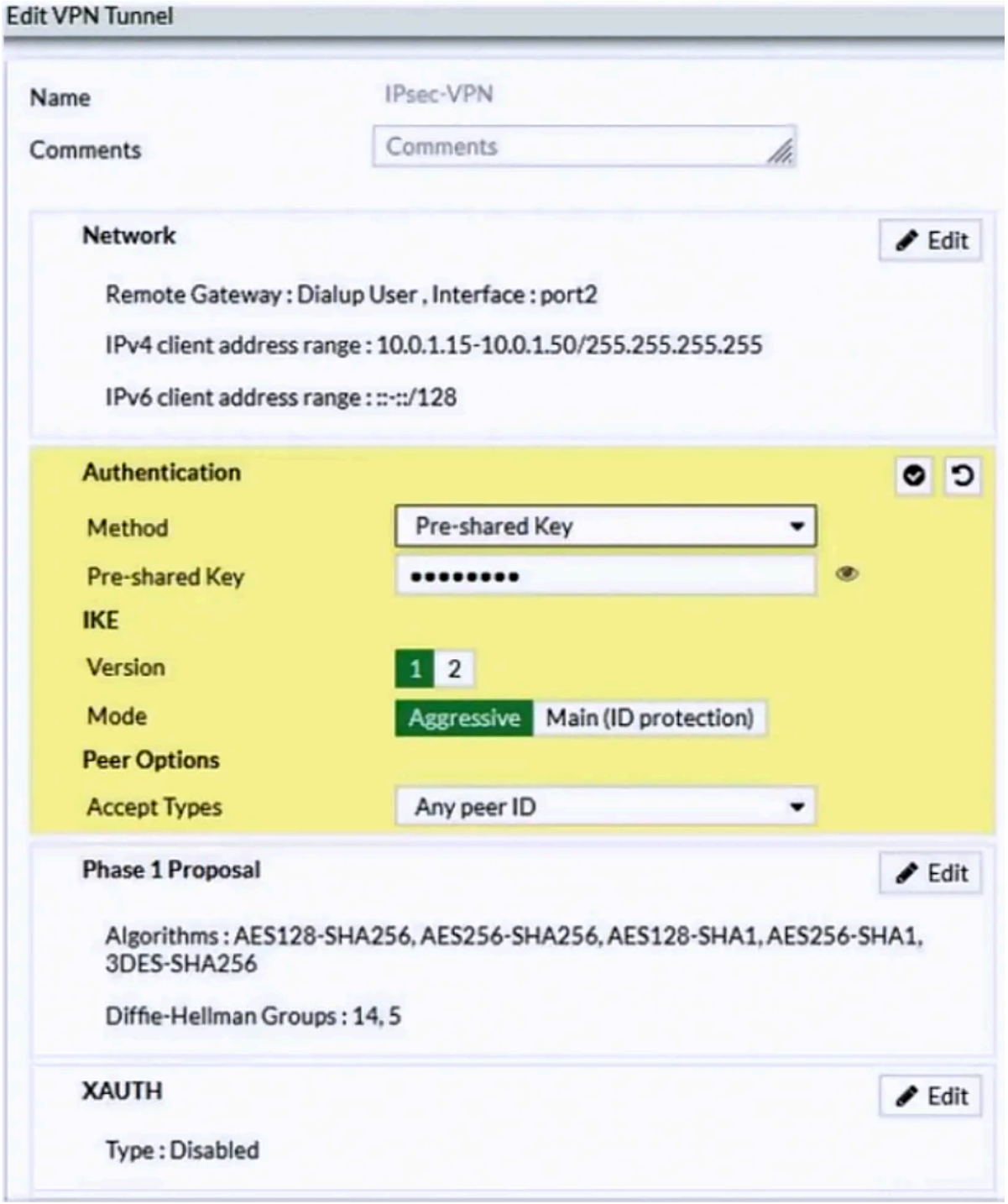
Wallsee 2 years ago

According to the FortiManager Administration Guide1, "To enable the SSID, you must select at least one channel for the radio. If no channels are selected, the SSID will not be enabled." Therefore, enabling one channel in the Channels section will allow the SSIDs to broadcast.

upvoted 2 times

Question #6 *Topic 1*

Refer to the exhibit.
Examine the IPsec VPN phase 1 configuration shown in the exhibit.
An administrator wants to use certificate-based authentication for an IPsec VPN user.
Which three configuration changes must you make on FortiGate to perform certificate-based authentication for the IPsec VPN user? (Choose three.)



A. Create a PKI user for the IPsec VPN user, and then configure the IPsec VPN tunnel to accept the PKI user as peer certificate.

B. In the Authentication section of the IPsec VPN tunnel, in the Method drop-down list, select Signature, and then select the certificate that FortiGate will use for IPsec VPN.

C. In the IKE section of the IPsec VPN tunnel, in the Mode field, select Main (ID protection).

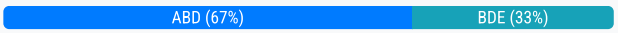
D. Import the CA that signed the user certificate.

E. Enable XAUTH on the IPsec VPN tunnel.

Suggested Answer: *A, B, D*

Official Answer: ABD

Community vote distribution



tonifan Most Recent 1 year, 4 months ago

abd are correct. XAUTH is spoken only in pag 46 about CHAP

upvoted 1 times

TheUsD 1 year, 8 months ago

ABD p. 79 study guide

upvoted 1 times

Artbrut 2 years, 5 months ago

p. 79 study guide

upvoted 2 times

aandreou020 2 years, 6 months ago

Sorry ABD

upvoted 1 times

aandreou020 2 years, 6 months ago

ADE are the correct answers!! For sure you need to create PKI User

upvoted 1 times

Wallsee 2 years, 6 months ago

Option A is false because creating a PKI user for the IPsec VPN user is not required, as the user certificate can be verified by the CA certificate.

upvoted 2 times

Question #7 *Topic 1*

You are investigating a report of poor wireless performance in a network that you manage. The issue is related to an AP interface in the 5 GHz range. You are monitoring the channel utilization over time.
What is the recommended maximum utilization value that an interface should not exceed?

A. 85%

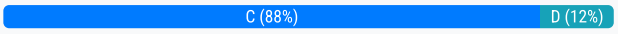
B. 95%

C. 75%

D. 65%

Suggested Answer: *D*
Official Answer: D

Community vote distribution



WontonSalad Most Recent 2 years, 1 month ago
p. 444 slide 54
upvoted 1 times

Artbrut 2 years, 5 months ago
p. 444
upvoted 2 times

FortiTorti 2 years, 5 months ago
C Page 444
upvoted 2 times

mollyk70 2 years, 5 months ago
C - Max rec - Utilization is 75%, P444 Study guide
upvoted 2 times

kinge2 2 years, 5 months ago
C is correct answer as per study guide page 444
upvoted 2 times

kinge2 2 years, 6 months ago
D is correct as Good signal on a Fortigate -> Wifi clients is 65dBm
upvoted 1 times

Question #8 *Topic 1*

Which CLI command should an administrator use to view the certificate verification process in real time?

A. diagnose debug application foauthd -1

B. diagnose debug application radiusd -1

C. diagnose debug application authd -1

D. diagnose debug application fnbamd -1

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

Artbrut 1 year, 11 months ago

Selected Answer: D

study guide p. 17

upvoted 1 times

Artbrut 1 year, 11 months ago

study guide p. 17sorry p. 90 study guide

upvoted 1 times

Artbrut Most Recent 1 year, 10 months ago

sorry p. 90 study guide

upvoted 1 times

mollyk70 1 year, 11 months ago

D - P17 Study Guide

upvoted 1 times

Question #9 *Topic 1*

Which two statements about the guest portal on FortiAuthenticator are true? (Choose two.)

A. Each remote user on FortiAuthenticator can sponsor up to 10 guest accounts.

B. Administrators must approve all guest accounts before they can be used.

C. The guest portal provides pre and post-log in services.

D. Administrators can use one or more incoming parameters to configure a mapping rule for the guest portal.

Suggested Answer: *C, D*

Official Answer: CD

Community vote distribution

CD (100%)

Artbrut Most Recent 1 year, 11 months ago

study guide p. 372, also read text below slide

upvoted 1 times

kinge2 2 years ago

page 372 and 380 of study guide

upvoted 1 times

Question #10 *Topic 1*

Refer to the exhibits.

In the wireless configuration shown in the exhibits, an AP is deployed in a remote site and has a wireless network (VAP) called Corporate deployed to it.

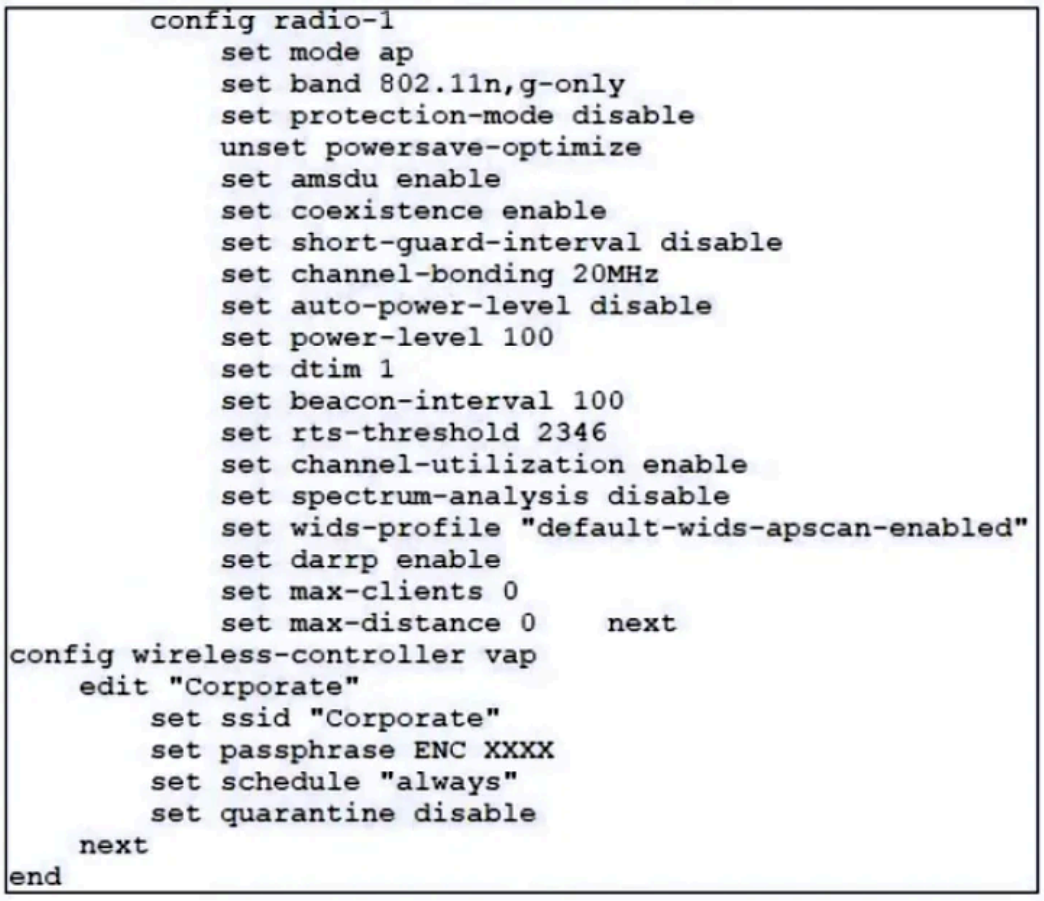
The network is a tunnelled network; however, clients connecting to a wireless network require access to a local printer. Clients are trying to print to a printer on the remote site, but are unable to do so.

Which configuration change is required to allow clients connected to the Corporate SSID to print locally?

Exhibit

```
config wireless-controller wtp-profile
    edit "Main Networks - FAP-320C"
        set comment "Profile with standard networks"
        config platform
            set type 320C
        end
        set wan-port-mode wan-only
        set led-state enable
        set dtls-policy clear-text
        set max-clients 0
        set handoff-rssi 30
        set handoff-sta-thresh 30
        set handoff-roaming enable
        set ap-country GB
        set ip-fragment-preventing tcp-mss-adjust
        set tun-mtu-uplink 0
        set tun-mtu-downlink 0
        set split-tunneling-acl-path local
        set split-tunneling-acl-local-ap-subnet enable
        config split-tunneling-acl
            edit 1
                set dest-ip 192.168.5.0 255.255.255.0
            next
        end
        set allowaccess https ssh
        set login-passwd-change yes
        set lldp disable
```

Exhibit



```
        config radio-1
            set mode ap
            set band 802.11n,g-only
            set protection-mode disable
            unset powersave-optimize
            set amsdu enable
            set coexistence enable
            set short-guard-interval disable
            set channel-bonding 20MHz
            set auto-power-level disable
            set power-level 100
            set dtim 1
            set beacon-interval 100
            set rts-threshold 2346
            set channel-utilization enable
            set spectrum-analysis disable
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable
            set max-clients 0
            set max-distance 0    next
config wireless-controller vap
    edit "Corporate"
        set ssid "Corporate"
        set passphrase ENC XXXX
        set schedule "always"
        set quarantine disable
    next
end
```

A. Configure split-tunneling in the vap configuration.

B. Configure split-tunneling in the wtp-profile configuration.

C. Disable the Block Intra-SSID Traffic (Intra-vap-privacy) setting on the SSID (VAP) profile.

D. Configure the printer as a wireless client on the Corporate wireless network.

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

JohnnyExam 1 year, 10 months ago

split-tunnel has to be configured both on vap and wtp-profile, but in this case the correct answer is A since it already has been enabled in wtp-profile according to configuration

upvoted 1 times

FortiTorti 1 year, 11 months ago

A - Page 323

upvoted 2 times

kinge2 2 years ago

A is correct as you need to enable split-tunelling on the vap SSID profile. This is also mentioned on page 323 of study guide

upvoted 2 times

aandreou020 2 years ago

Answer B is correct . Split tunnel can be enable on the profile

upvoted 1 times

aandreou020 2 years ago

Answer B is correct . Split tunnel can be enable on the profileit already is enabled in wtp-profile, according to configuration above, so the correct answer is A where it still needs to be enabled

upvoted 1 times

JohnnyExam Most Recent 1 year, 10 months ago

it already is enabled in wtp-profile, according to configuration above, so the correct answer is A where it still needs to be enabled

upvoted 1 times

Question #11 *Topic 1*

Which EAP method requires the use of a digital certificate on both the server end and the client end?

A. EAP-TTLS

B. PEAP

C. EAP-GTC

D. EAP-TLS

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

gbrodrigues Most Recent 1 year, 5 months ago

given answer is correct.

upvoted 1 times

kinge2 2 years ago

page 262 of study guide

upvoted 2 times

Question #12 *Topic 1*

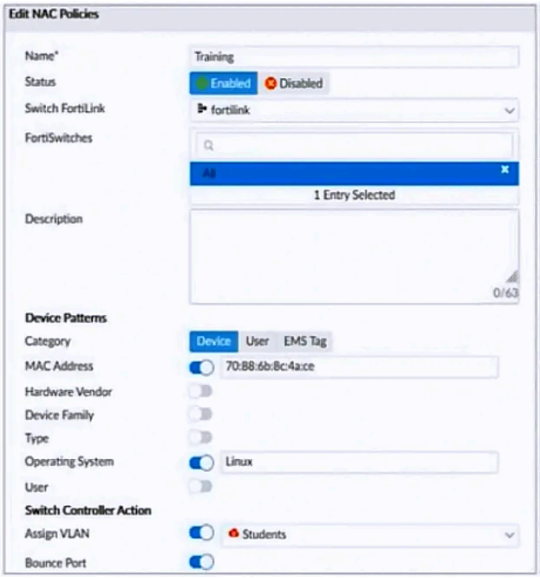
Refer to the exhibit.

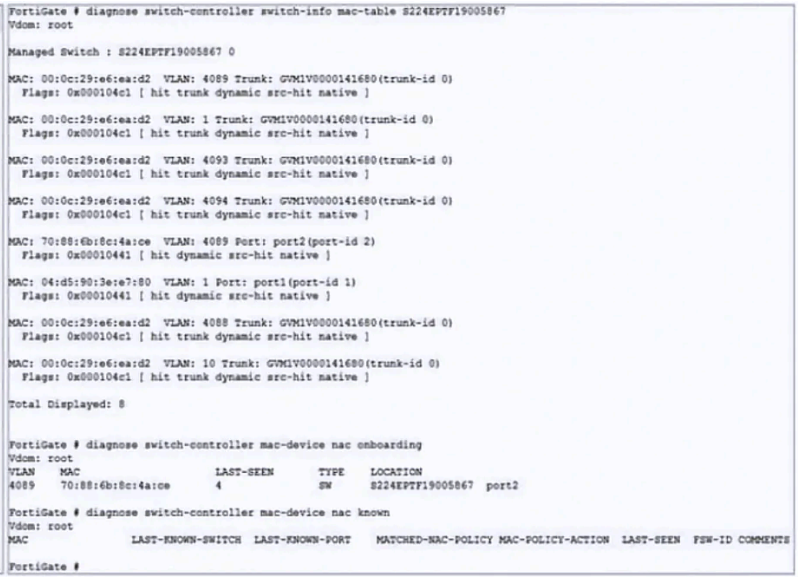
Examine the FortiManager configuration and FortiGate CLI output shown in the exhibit.

An administrator is testing the NAC feature. The test device is connected to a managed FortiSwitch device (S224EPTF19005867) on port2.

After applying the NAC policy on port2 and generating traffic on the test device, the test device is not matching the NAC policy; therefore, the test device remains in the onboarding VLAN.

Based on the information shown in the exhibit, which two scenarios are likely to cause this issue? (Choose two.)





A. Management communication between FortiGate and FortiSwitch is down.

B. The MAC address configured on the NAC policy is incorrect.

C. The device operating system detected by FortiGate is not Linux.

D. Device detection is not enabled on VLAN 4089.

Suggested Answer: *B, C*

Official Answer: BC

Community vote distribution

CD (60%) BC (20%) AB (20%)

_zero Most Recent 1 year, 7 months ago

Correct answer are C & D. A it's not correct because if the communication is down the FortiGate can't retrieve the switch information, and B it's not correct to, because both exhibit have the same mac-address.

upvoted 1 times

Artbrut 1 year, 11 months ago

Selected Answer: CD

unsure, but we don´t know if device detection is enabled on switch-controller and which OS the device is.

https://docs.fortinet.com/document/fortiswitch/7.0.8/devices-managed-by-fortios/801195/enabling-network-assisted-device-detection

upvoted 2 times

Artbrut 1 year, 11 months ago

unsure, but we don´t know if device detection is enabled on switch-controller and which OS the device is.

https://docs.fortinet.com/document/fortiswitch/7.0.8/devices-managed-by-fortios/801195/enabling-network-assisted-device-detectionStudy guide p. 229 - enable device detectionhttps://docs.fortinet.com/document/fortiswitch/7.4.2/fortilink-guide/173271/fortiswitch-network-access-control To show known NAC devices with a known location that match a NAC policy: diagnose switch-controller mac-device nac known To show pending NAC devices with an unknown location that match a NAC policy: diagnose switch-controller mac-device nac onboarding --> so I think it is B and C as the cli output shows, that the MAC address is known as a NAC device

upvoted 2 times

Artbrut 1 year, 10 months ago

Study guide p. 229 - enable device detection

upvoted 1 times

Artbrut 1 year, 10 months ago

Study guide p. 229 - enable device detectionhttps://docs.fortinet.com/document/fortiswitch/7.4.2/fortilink-guide/173271/fortiswitch-network-access-control To show known NAC devices with a known location that match a NAC policy: diagnose switch-controller mac-device nac known To show pending NAC devices with an unknown location that match a NAC policy: diagnose switch-controller mac-device nac onboarding --> so I think it is B and C as the cli output shows, that the MAC address is known as a NAC device

upvoted 1 times

Artbrut 1 year, 10 months ago

https://docs.fortinet.com/document/fortiswitch/7.4.2/fortilink-guide/173271/fortiswitch-network-access-control To show known NAC devices with a known location that match a NAC policy: diagnose switch-controller mac-device nac known To show pending NAC devices with an unknown location that match a NAC policy: diagnose switch-controller mac-device nac onboarding --> so I think it is B and C as the cli output shows, that the MAC address is known as a NAC device

upvoted 1 times

kinge2 2 years ago

A incorrect because user wont be able to connect to port2 and generate traffic unless it is an unmanaged switch.

upvoted 1 times

Wallsee 2 years ago

Option A is also true because the FortiSwitch device status is shown as down, which means that the management communication between FortiGate and FortiSwitch is not working properly. This could prevent the NAC policy from being applied correctly. Option C is false because the device operating system detected by FortiGate is Linux, which matches the NAC policy.

upvoted 1 times

Question #13 *Topic 1*

Which two pieces of information can the diagnose test authserver ldap command provide? (Choose two.)

A. It displays whether the admin bind user credentials are correct.

B. It displays whether the user credentials are correct.

C. It displays the LDAP codes returned by the LDAP server.

D. It displays the LDAP groups found for the user.

Suggested Answer: *A, C*

Official Answer: AC

Community vote distribution

BD (100%)

tonifan Most Recent 1 year, 4 months ago

Answer B D !! Study Guide P16

upvoted 1 times

Artbrut 1 year, 11 months ago

study guide p. 16

upvoted 2 times

FortiTorti 1 year, 11 months ago

B D - Page 16

upvoted 2 times

kinge2 2 years ago

study guide p16

upvoted 2 times

aandreou020 2 years ago

Answer B D !! Study Guide P16

upvoted 3 times

Question #14 *Topic 1*

You are setting up an SSID (VAP) to perform RADIUS-authenticated dynamic VLAN allocation.
Which three RADIUS attributes must be supplied by the RADIUS server to enable successful VLAN allocation? (Choose three.)

A. Tunnel-Private-Group-ID

B. Tunnel-Pvt-Group-ID

C. Tunnel-Preference

D. Tunnel-Type

E. Tunnel-Medium-Type

Suggested Answer: *A, D, E*
Official Answer: ADE

Community vote distribution
BDE (100%)

Cesar12345 Most Recent 1 year, 9 months ago
Study guide says BDE but IETF says Tunnel-Private-Group-ID ...
upvoted 1 times

Artbrut 1 year, 11 months ago
page 340 study guide
upvoted 1 times

FortiTorti 1 year, 11 months ago
BDE - Page 340
upvoted 1 times

aandreou020 2 years ago
Answer BDE are correct
upvoted 1 times

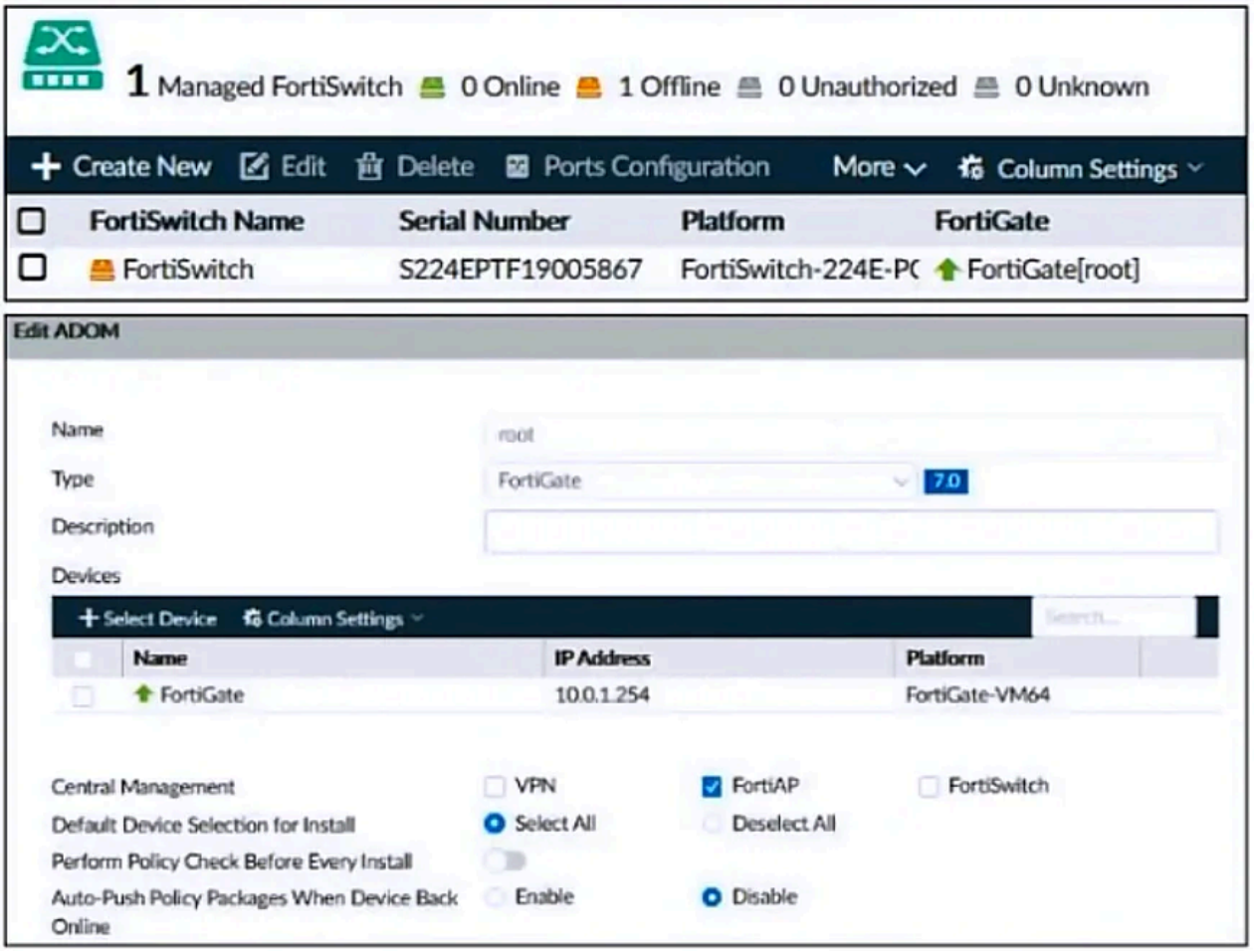
certificationsuptodate 2 years ago
Study guide pag.340
upvoted 2 times

Question #15 *Topic 1*

Refer to the exhibit.

Examine the FortiManager information shown in the exhibit.

Which two statements about the FortiManager status are true? (Choose two.)



A. FortiSwitch manager is working in per-device management mode.

B. FortiSwitch is not authorized.

C. FortiSwitch manager is working in central management mode.

D. FortiSwitch is authorized and offline.

Suggested Answer: *A, D*

Official Answer: AD

Community vote distribution

AD (100%)

Artbrut Most Recent 1 year, 11 months ago

study guide p. 174/175

upvoted 2 times

mollyk70 1 year, 11 months ago

AD Correct Study guide 174 A-Clear FortiSwitch button to enable per device mgmt D-FortiSwitch is clearly Offline

upvoted 2 times

kinge2 2 years ago

switch central mgmt not enabled

upvoted 2 times

Question #16 *Topic 1*

An administrator is testing the connectivity for a new VLAN. The devices in the VLAN are connected to a FortiSwitch device that is managed by FortiGate. Quarantine is disabled on FortiGate.
While testing, the administrator noticed that devices can ping FortiGate and FortiGate can ping the devices. The administrator also noticed that inter-VLAN communication works. However, intra-VLAN communication does not work.
Which scenario is likely to cause this issue?

A. The native VLAN configured on the ports is incorrect.

B. The FortiSwitch MAC address table is missing entries.

C. The FortiGate ARP table is missing entries.

D. Access VLAN is enabled on the VLAN.

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

Artbrut Most Recent 1 year, 11 months ago
page 224
upvoted 1 times

kinge2 2 years ago
page 224 of study guide
upvoted 1 times

Question #17 *Topic 1*

Refer to the exhibit.

By default, FortiOS creates the following DHCP server scope for the FortiLink interface as shown in the exhibit.

What is the objective of the vci-string setting?

```
config system dhcp server
    edit 1
        set ntp-service local
        set default-gateway 169.254.1.1
        set netmask 255.255.255.0
        set interface "fortilink"
        config ip-range
            edit 1
                set start-ip 169.254.1.2
                set end-ip 169.254.1.254
            next
        end
        set vci-match enable
        set vci-string "FortiSwitch" "FortiExtender"
    next
end
```

A. To ignore DHCP requests coming from FortiSwitch and FortiExtender devices

B. To reserve IP addresses for FortiSwitch and FortiExtender devices

C. To restrict the IP address assignment to FortiSwitch and FortiExtender devices

D. To restrict the IP address assignment to devices that have FortiSwitch or FortiExtender as their hostname

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

tonifan Most Recent 1 year, 4 months ago

confermo la C a pagina 209

upvoted 1 times

Artbrut 1 year, 11 months ago

C, as per p. 209 study guide

upvoted 1 times

kinge2 2 years ago

page 209 of study guide

upvoted 1 times